2^n - 21,382,107,400,956,509,849 IS NEVER A PRIME

Joel Spencer

October 1969

P-4229

2^n - 21,382,107,400,956,509,949 is never a prime

Joel Spencer*

The Rand Corporation, Santa Monica, California

The sequence $2^n - a$ for fixed a has been studied by many mathematicians. For a = +1, those $2^n - 1$ which are primes are called Mersenne primes. For a = -1, the primes of the form $2^n + 1$ are called Fermat primes. Clearly if a is even the only possible prime would be 2. In this note, I find an odd a such that $2^n - a$ is never a prime.

If p is a prime set $x(p) =$ minimal $t > 0$: $2^t \equiv 1 \pmod{p}$. So given x(p) we must have $p \mid 2^{x(p)} - 1$ and $p \nmid 2^t - 1$ for $1 < t < p$. If x(p) is even then $p \nmid 2^{\frac{x(p)}{2}} - 1$ implies $p \mid 2^{\frac{x(p)}{2}} + 1$. It is not difficult to show $x(p) = 2^i$ iff $p \mid 2^{2^{i-1}} + 1$. We get the table:

---

*Any views expressed in this paper are those of the author. They should not be interpreted as reflecting the views of The Rand Corporation or the official opinion or policy of any of its governmental or private research sponsors. Papers are reproduced by The Rand Corporation as a courtesy to members of its staff.

$x(p)$	$2^{x(p)/2}+1$	p
2	3	3
4	5	5
8	17	17
16	257	257
32	65537	65537
64	4,294,967,297	641,6700417

The last row gives the factorization of $2^{32}+1$ first found by Fermat. Now the equation $2^n \equiv a(p)$ will either have no solutions or the solution set $n \equiv b(x(p))$ where $2^b \equiv a(p)$. Thus if $a \equiv -1(3)$, $2^n \equiv a(3)$ iff $n \equiv 1(2)$. We have $-1 \equiv 2^{x(p)/2}(p)$ whenever $x(p)$ is even. Set

$$a \equiv -1\ [3,5,17,257,65537,641].$$

Then

$$\begin{aligned}
2^n &\equiv a\ (3) \text{ iff } n \equiv 1(2)\\
2^n &\equiv a\ (5) \text{ iff } n \equiv 2(4)\\
2^n &\equiv a\ (17) \text{ iff } n \equiv 4(8)\\
2^n &\equiv a\ (257) \text{ iff } n \equiv 8(16)\\
2^n &\equiv a(65537) \text{ iff } n \equiv 16(32)\\
2^n &\equiv a\ (641) \text{ iff } n \equiv 32(64)
\end{aligned}$$

If

$$a \equiv +1[6700417]$$

$$2^n \equiv a(6700417) \text{ iff } n \equiv 0(64).$$

By the Chinese Remainder Theorem we may solve for a modulo 3.5.17.257.65537.641.6700417. A solution is given as the title. Note all n's satisfy exactly one of the consequences given so all $2^n - a$ are divisible by 3,5,17,257,65537, or 6700417. One can easily check that $|2^n - a| > 10^{15}$ for all n so it never equals one of these primes.

The following result is due to O. 144.

Corollary: There exist infinitely many primes p such that $2^n - p$ is never a prime.

Proof: If $a \equiv a_o \pmod{\Delta}$ when a_o is given in the title and Δ is the product of the primes then $2^n - a$ is always divisible by one of the seven primes. By Dirichlet's Theorem that residue class contains an infinite number of primes. Taking a negative and large $2^n - a$ never equals any of the primes so is never a prime.